RECEIVED
CENTRAL FAX CENTER
DEC 07 2006

CLAIM AMENDMENTS

1.(Currently amended) A method for biometrically securing access to an electronic system, said method comprising the steps of:

obtaining identification of a user from a smart card presented to the electronic system by said user;

~~using a computer network to obtain~~ accessing a user profile including biometric attributes associated with said user from ~~a server~~ said smart card;

prompting ~~a~~ said user to input to a biometric user interface associated with said electronic system at least one biometric attribute randomly selected from said user profile containing biometric attributes of said user; and

permitting said user to perform a user-desired activity with the electronic system[,] if at least one biometric attribute input by said user to said biometric user interface associated with said electronic system matches said at least one biometric attribute randomly selected from said user profile.

2.(Previously presented) The method of claim 1 wherein said computer network is a secure computer network.

3.(Previously presented) The method of claim 1 wherein said user profile is stored in a biometric broker.

4.(Previously presented) The method of claim 1 further comprising the steps of:

obtaining at least one biometric attribute from said user for compilation in said user profile; compiling said user profile; and

storing said user profile in said server accessible by at least one biometric user interface associated with said electronic system.

5.(Original) The method of claim 4 further comprising the step of:

permitting said user to modify said user profile, in response to approval of a request by said user.

6.(Previously presented) The method of claim 1 further comprising the step of:

comparing at least one biometric attribute input by said user to said biometric user interface associated with said electronic system with said at least one biometric attribute randomly selected from said user profile.

7.(Previously presented) The method of claim 6 further comprising the step of:

subsequently prompting a user to input to said biometric user interface associated with said electronic system at least one additional biometric attribute randomly selected from said user profile, if at least one biometric attribute previously input by said user to said biometric user interface associated with said electronic system does not match said at least one biometric attribute previously randomly selected from said user profile.

8.(Original) The method of claim 1 wherein said electronic system comprises at least one wireless device that operates with a wireless network.

9.(Original) The method of claim 1 wherein said electronic system comprises at least one computer workstation operable over an associated network.

10.(Original) The method of claim 1 wherein said electronic system comprises an automated teller machine.

11.(Original) The method of claim 1 wherein said electronic system comprises a secured entry system to a secured environment.

12.(Original) The method of claim 1 wherein said electronic system comprises a wireless network.

13. (Canceled)

14.(Original) The method of claim 1 wherein said electronic system comprises a wireless device.

15.(Previously presented) The method of claim 1 further comprising the steps of:

identifying at least one defective biometric attribute associated with said user; and thereafter prompting a user to input to said biometric user interface associated with said electronic system at least one additional biometric attribute randomly selected from said user profile containing biometric attributes of said user.

16.(Original) The method of claim 1 wherein said user-desired activity comprises a financial transaction.

17.(Original) The method of claim 1 wherein said user-desired activity comprises an ATM transaction.

18.(Original) The method of claim 1 wherein said user-desired activity comprises access to a secure area.

19.(Original) The method of claim 1 wherein said user-desired activity comprises access to data from said electronic system.

20.(Original) The method of claim 1 wherein said user-desired activity comprises execution of a mechanical activity.

21.(Original) The method of claim 1 further comprising the step of:

initiating access to said electronic system utilizing only one biometric attribute input to said electronic system.

22.(Currently amended) A method for biometrically securing access to an electronic system, said method comprising the steps of:

obtaining identification of a user from a smart card presented to the electronic system by said user;

based on said identification, using a computer network to obtain a user profile associated with said user from a remote server said user profile including biometric attributes;

~~using a computer network to obtain a user profile from a server;~~

prompting a user to input to a biometric user interface associated with said electronic system at least two biometric attributes randomly selected from said user profile containing biometric attributes of said user; and

permitting said user to perform a user-desired activity at said electronic system[,] if biometric attributes input by said user to said biometric user interface associated with said electronic system matches said at least two biometric attribute randomly selected from said user profile.

23.(Currently amended) A system for biometrically securing access to an electronic system, said system comprising:

an electronic system adapted to permit a user to perform a user-desired activity if at least one biometric attribute input by the user to said biometric user interface matches said at least one biometric attribute randomly selected from a user profile accessible by the electronic system from a smart card presented to the electronic system by the user, ~~server a computer network~~, wherein said smart card is adapted to store at least one user profile including biometric attributes[,] and ~~capable of allowing at least one biometric user interface associated with~~ provide said electronic system ~~also connected to said computer network to~~ access to said at least one user profile;

a smart card reader associated with said electronic system; and

a biometric user interface associated with said electronic system ~~and connected to said computer network that accesses a user profile stored on said server that contains biometric attributes of said user and that prompts~~ adapted to enable said user to input at least one biometric to said electronic system for comparison to at least one biometric attribute randomly selected by said electronic system from said user profile; [and]

wherein said ~~an~~ electronic system is adapted to permit ~~for permitting~~ said user to perform a user-desired activity, if at least one biometric attribute input by said user to said

biometric user interface matches said at least one biometric attribute randomly selected from said user profile by said electronic system.

24.(Cancelled).

25.(Previously presented) The system of claim 23 wherein said user profile is accessible from a biometric broker via a secure network connection.

26.(Previously presented) The system of claim 23 wherein: at least one biometric attribute is obtained from said user for compilation in said user profile.

27.(Previously presented) The system of claim 23 wherein said user is permitted to modify said user profile, in response to approval of a request by said user.

28.(Previously presented) The system of claim 23 further comprising:

module for comparing at least one biometric attribute input by said user to said biometric user interface associated with said electronic system with said at least one biometric attribute randomly selected from said user profile.

29.(Previously presented) The system of claim 28 further comprising:

module for subsequently prompting said user to input to said biometric user interface associated with said electronic system at least one additional biometric attribute randomly selected from said user profile, if at least one biometric attribute previously input by said user to said biometric user interface associated with said electronic system does not match said at least one biometric attribute randomly previously selected from said user profile.

30.(Original) The system of claim 23 wherein said electronic system comprises at least one wireless device that operates with a wireless network.

31.(Currently amended) The system of claim 23 wherein said electronic system comprises at least one computer workstation accessible over said computer network.

32.(Original) The system of claim 23 wherein said electronic system comprises an automated teller machine.

33.(Original) The system of claim 23 wherein said electronic system comprises a secured entry system to a secured environment.

34.(Previously amended) The system of claim 23 wherein said computer network comprises a wireless network.

35.(Cancelled).

36.(Original) The system of claim 23 wherein said electronic system comprises a wireless device.

37.(Previously presented) The system of claim 23 further comprising:

module for identifying at least one defective biometric attribute associated with said user; and

wherein said user is thereafter prompted to input to said electronic system at least one additional biometric attribute randomly selected from a user profile containing biometric attributes of said user.

38.(Original) The system of claim 23 wherein said user-desired activity comprises a financial transaction.

39.(Original) The system of claim 23 wherein said user-desired activity comprises an ATM transaction.

40.(Original) The system of claim 23 wherein said user-desired activity comprises access to a

secure area.

41.(Original) The system of claim 23 wherein said user-desired activity comprises access to data from said electronic system.

42.(Original) The system of claim 23 wherein said user-desired activity comprises execution of a mechanical activity.

43. (Original) The system of claim 23 wherein access to said electronic system is initiated utilizing only one biometric attribute input to said electronic system.

44.(Currently amended) A system for biometrically securing access to an electronic system, said system comprising:

an electronic system adapted to permit a user to perform a user-desired activity if at least one biometric attribute input by the user to said biometric user interface matches said at least one biometric attribute randomly selected from said user profile accessible by the electronic system over a computer network from a remote server, said electronic system including access to a remote server ~~connected to~~ through electronic connection to a computer network ~~that is~~, and said remote server adapted to store at least one user profile including biometric attributes[,] and ~~is capable of allowing at least one biometric user interface associated with~~ provide said electronic system ~~and connected to said computer network to~~ access to said at least one user profile;

a smart card reader associated with said electronic system; and

a biometric user interface associated with said electronic system ~~and connected to said computer network that accesses a user profile stored on said server that contains biometric attributes of said user and that prompts~~ adapted to enable said user to input at least one biometric to said biometric user interface for comparison to at least two biometric attributes randomly selected by said electronic system from said user profile; [and]

wherein said ~~an~~ electronic system is adapted to permit ~~for permitting~~ said user to perform a user-desired activity, if at least one biometric attribute input by said user to said biometric user interface matches said at least one biometric attribute randomly selected from said user profile by said electronic system.